PN - JP9223210 A 19970826

PD - 1997-08-26

PR - JP19960053646 19960219

OPD - 1996-02-19

TI - PORTABLE INFORMATION STORAGE MEDIUM AND AUTHENTICATION METHOD AND AUTHENTICATION SYSTEM USING THE SAME

IN - HAYASHI MASAHIRO

PA - DAINIPPON PRINTING CO LTD

IC - G06K17/00 ; G06F1/00 ; G09C1/00 ; H04L9/32 ; G07F7/08

TI - Portable data recording medium authentication method for commercial transaction - by obtaining digital signature that includes open key and secret key used in authentication operation of public key cryptic system, from portable data recording medium

PR - JP19960053646 19960219

PN - JP9223210 A 19970826 DW199744 G06K17/00 007pp

PA - (NIPQ) DAINIPPON PRINTING CO LTD

IC - G06F1/00 ;G06K17/00 ;G07F7/08 ;G09C1/00 ;H04L9/32

AB - J09223210 The method entails obtaining a digital signature from a portable data recording medium (10) such as an integrated circuit card. The digital signature includes an open key (2) and a secret key (1) which are used in an authentication operation of a public key cryptic system.

- ADVANTAGE - Safely manages key used in authenticating digital signature since unauthorised usage and alterations are prevented. Keeps key in portable data recording medium thereby eliminating need to store key in magnetic disk of network terminal.

- (Dwg.2/5)

OPD - 1996-02-19

AN - 1997-476960 [44]

PN - JP9223210 A 19970826

PD - 1997-08-26

AP - JP19960053646 19960219

IN - HAYASHI MASAHIRO

PA - DAINIPPON PRINTING CO LTD

TI - PORTABLE INFORMATION STORAGE MEDIUM AND AUTHENTICATION METHOD AND AUTHENTICATION SYSTEM USING THE SAME

AB - PROBLEM TO BE SOLVED: To safely and efficiently manage a secret key and a public key by housing at least a pair of the public key and the secret key used for the authentication of a public key ciphering system as a public key certificate composed of the public key and the digital signature of a notarial jnstitution for the public key and the secret key.

- SOLUTION: In an IC card10 being a portable information recording medium, at least a pair of the public key and the secret key used for the authentication of the public key ciphering system are housed as the public key certificate composed of the public key and the digital signature of the notarial institution for the public key and the secret key. When Taro sends a message to Jiro, the IC card10 housing the secret key or the like is obtained from a CA (notarial institution) 7 and the digital signature and the public key certificate are added and sent. The authentication server 7 of the notarial institution is provided with the data base of the public key (of Taro and Jiro or the like) and an IC card reader-writer8 for issuing the IC card 10. Also, the terminals 9 of Taro and Jiro are also provided with the IC card reader-writer 8.

SI - G07F7/08

I - G06K17/00 ;G06F1/00 ;G09C1/00 ;G09C1/00 ;G09C1/00 ;H04L9/32

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平9－223210

(43)公開日　平成９年(1997)８月26日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｋ　17/00			Ｇ０６Ｋ　17/00	Ｔ	
Ｇ０６Ｆ　1/00	３７０		Ｇ０６Ｆ　1/00	３７０Ｅ	
Ｇ０９Ｃ　1/00	６２０	7259－5Ｊ	Ｇ０９Ｃ　1/00	６２０Ｂ	
	６４０	7259－5Ｊ		６４０Ｂ	
		7259－5Ｊ		６４０Ｅ	

審査請求　未請求　請求項の数９　ＦＤ　（全７頁）　最終頁に続く

(21)出願番号　特願平8－53646

(22)出願日　平成８年(1996)２月19日

(71)出願人　000002897
大日本印刷株式会社
東京都新宿区市谷加賀町一丁目１番１号

(72)発明者　林　昌弘
東京都新宿区市谷加賀町一丁目１番１号
大日本印刷株式会社内

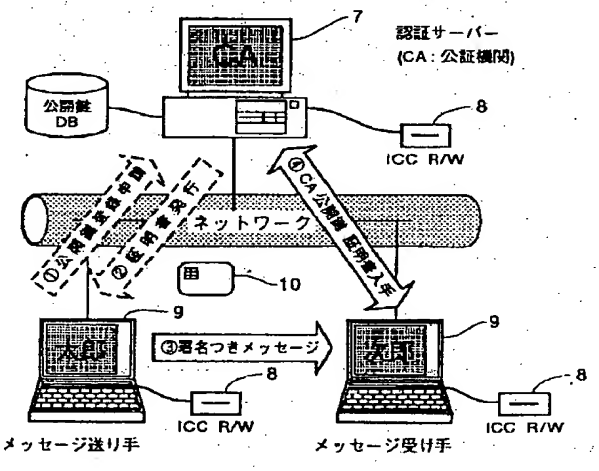
(74)代理人　弁理士　小西　淳美

(54)【発明の名称】　携帯可能情報記憶媒体及びそれを用いた認証方法、認証システム

(57)【要約】

【課題】　ネットワークでデジタル署名署等の認証に用いる鍵を安全に管理する。

【解決手段】　ＲＳＡ署名法等の公開鍵暗号方式の認証に用いる、公開鍵及び秘密鍵を、公開鍵及び該公開鍵に対するＣＡ（公証機関）のデジタル署名とからなる公開鍵証明書と、秘密鍵として収容したＩＣカードを用いる。送り手はＣＡからオフラインで入手したＩＣカードをネットワーク端末にセットして、秘密鍵でデジタル署名を作成し、メッセージにデジタル署名と公開鍵証明書とを添付して受け手に送る。受け手では、別途用意したＣＡの公開鍵で、送られた公開鍵証明書のＣＡの署名を認証し、送り手の公開鍵を認証する。認証された送り手の公開鍵で送り手の署名を認証し、メッセージを認証する。



【特許請求の範囲】
【請求項１】　公開鍵暗号方式の認証に用いる少なくとも一対の公開鍵及び秘密鍵を、公開鍵及び該公開鍵に対する公証機関のデジタル署名とからなる公開鍵証明書と、秘密鍵として収容した、携帯可能情報記憶媒体。
【請求項２】　収容された秘密鍵が外部読出禁止属性を有し、外部より入力された原文を該秘密鍵を用いて媒体内部で暗号化して暗号文を出力する、請求項１記載の携帯可能情報記憶媒体。
【請求項３】　収容された公開鍵証明書が書換禁止属性を有する請求項１又は２記載の記載の携帯可能情報記憶媒体。
【請求項４】　携帯可能情報記憶媒体がＣＰＵとメモリを有するＩＣカードである、請求項１～３のいずれか１項に記載の携帯可能情報記憶媒体。
【請求項５】　収容された公開鍵及び秘密鍵が、ＲＳＡ署名法によるデジタル署名に用いる復号鍵及び暗号鍵である、請求項１～４のいずれか１項に記載の携帯可能情報記憶媒体。
【請求項６】　ネットワークで送り手が受け手に情報を送付する際に該情報の認証情報として利用する公開鍵暗号方式の公開鍵及び秘密鍵について、送り手は公証機関から請求項１～４のいずれかに記載の携帯可能情報記憶媒体を取得する事で、公開鍵及び該公開鍵に対する公証機関のデジタル署名とからなる公開鍵証明書と、秘密鍵とを用意し、
送り手は受け手に上記秘密鍵で作成した認証情報とともに、上記公開鍵証明書を送付し、
受け手では、用意した公証機関の公開鍵と、送り手から送付された公開鍵証明書が有する公証機関のデジタル署名とを用いて、先ず該公開鍵証明書が有する送り手の公開鍵を認証し、次いで該認証された送り手の公開鍵と送り手から送付された認証情報とを用いて送付された情報を認証する、携帯可能情報記憶媒体を用いた認証方法。
【請求項７】　認証情報がＲＳＡ署名法によるデジタル署名である請求項６記載の携帯可能情報記憶媒体を用いた認証方法。
【請求項８】　送り手が受け手に情報を送付する際に、該情報に添付する認証情報に公開鍵暗号方式の公開鍵及び秘密鍵を用いる、ネットワークシステムの認証システムにおいて、
少なくとも送り手の端末は、上記公開鍵及び秘密鍵について、公開鍵及び該公開鍵に対する公証機関のデジタル署名とからなる公開鍵証明書と、秘密鍵とを収容する請求項１～４のいずれかに記載の携帯可能情報記憶媒体を備え、
送り手は、該携帯可能情報記憶媒体に収容された上記秘密鍵を用いて作成された認証情報と、該携帯可能情報記憶媒体に収容された上記公開鍵証明書を送付する、携帯可能情報記憶媒体を用いた認証システム。
【請求項９】　認証情報がデジタル署名である請求項８記載の携帯可能情報記憶媒体を用いた認証システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、ネットワークにおける情報伝達の際に、認証に利用する鍵の管理をより安全に行う技術に関する。特に、デジタル署名等の認証に利用する公開鍵暗号方式の秘密鍵及び公開鍵を安全且つ効率的に管理する技術に関する。
【０００２】
【従来の技術】近年、ネットワークが情報伝達手段として普及し、ネットワーク上での商取引等のさらなる展開において、伝達する情報の正当性を担保できる技術が極めて重要な事項となっている。例えば、認証情報としてデジタル署名を添付する方法がある。図３はデジタル署名の説明図である。デジタル署名とは、メッセージの送り手がメッセージに添付する一種の証明書である。また、いわば従来の紙に対する捺印である。デジタル署名は、通常、メッセージ（原文）を圧縮した圧縮文を送り手の暗号鍵で暗号化した暗号文であり（なお、暗号化の対象となる原文はメッセージの全て又は一部でも良い。）、送り手の復号鍵で元の圧縮文に復号できる。つまり、受け手は、受け取ったメッセージから圧縮文を作成し、また受け取ったデジタル署名を復号化してもう一つの圧縮文を作り、これら二つの圧縮文が一致する事で受け取ったメッセージの内容が改ざんされてなく正しいものであると判断する。また、デジタル署名は、そのメッセージが確かに送り手本人によって作成されたものである事を証明するものでもある。すなわち、デジタル署名は、紙ベースであれば、伝達すべきメッセージが記載された通知書に捺印された送り手の印鑑（の印影）であり、記載された内容の正当性と、記載内容が送り手によって作成されたものであると示すものである。従って、デジタル署名は、メッセージ認証とユーザ認証の両方の機能を有する。
【０００３】ところで、暗号鍵と復号鍵とが同一の鍵、すなわち対象暗号の場合は送り手及び受け手が用いる鍵の両方を秘密鍵（秘密鍵暗号方式）とする必要がある。しかし、暗号鍵と復号鍵とが異なる非対称暗号の場合は、何方か一方のみを秘密鍵として他方を公表する公開鍵とすることができる（公開鍵暗号方式）。このような非対称暗号の一つとして、ＲＳＡ（Ｒｉｖｅｓｔ，Ｓｈａｍｉｒ，Ａｄｅｌｍａｎ）暗号系がある。ＲＳＡ暗号系は、一般に、暗号鍵を公開鍵に復号鍵を秘密鍵にするが、デジタル署名にＲＳＡ暗号系を用いる場合は、暗号鍵を秘密鍵に復号鍵を公開鍵にする。これをＲＳＡ署名法という。こうすれば、送り手が暗号化に用いる自分の鍵を秘密鍵として安全に保管すれば良く、その秘密鍵に対する復号鍵は公開鍵として公表しても安全だからである。これは、紙ベースで、実印を自分で安全に保管すれ

ば良いのと同じである。

【０００４】ところで、紙ベースでも、捺印された印鑑（実印）の印影が送り手本人のものであることの確かな証明は、その実印の印影を有する印鑑（登録）証明書という、公的機関によって発行された書類によって印鑑証明がなされる。従って、実印を捺印した書類と、その実印が本人のものであるとことを証明する印鑑証明書が１セットになって、始めて、前記書類の正当性が確認される。これと同じ様に、デジタル署名でも、復号鍵を公開鍵とするには、信頼できる機関、すなわち公証機関（ＣＡ：Ｃｅｒｌｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ）が、その公開鍵を送り手本人のものに間違いないことを証明する手段が必要である。それが、公開鍵の証明書である。ところで、この公証機関による公開鍵証明書も、その公開鍵を一つの情報として捉えて、その情報（公開鍵）と、その情報に対する公証機関のデジタル署名とからなる。従って、送り手が受け手に送る、メッセージが今度は公開鍵であり、送り手が公証機関の場合に相当する。公証機関は、公証機関の秘密鍵で公証機関のデジタル署名を作成し、その公開鍵証明書を構成する公開鍵は、前記「公証機関の秘密鍵」と組の「公証機関の公開鍵」を用いて復号化して、認証することとなる。従って、送り手が受け手にメッセージ等の情報を送る際は、メッセージと共に、そのメッセージに対する送り手のデジタル署名と、そのデジタル署名からメッセージを認証する為の復号鍵と、その復号鍵が送り手本人のものであることを証明する公証機関の証明書（この証明書に前記復号鍵が含まれる）とを、送ることとなる。

【０００５】

【発明が解決しようとする課題】ところが、ＲＳＡ等の公開鍵暗号方式を認証に用いる場合、先ず自分の秘密鍵は厳重に管理することが必要だが、それをハードディスク或いはフロッピーディスク等の磁気ディスク等へ保管しても、第三者に不正にアクセスされ盗用や改ざんの危険性がある。また、復号鍵とする公開鍵は、公表する鍵のため盗用という問題はないが、改ざんに対しても公証機関の公開鍵証明書を取っておけば防御できる。しかし、取得した公開鍵証明書も秘密鍵と同様に磁気ディスク等に保管したものに不正にアクセスされて保管者の知らない内に改ざんされれば、証明書として機能しない。すなわち、受け手には不正な公開鍵証明書が送付される事になり、不正な証明書である事は判断できても、真正なものが送付されていないので、結局、送り手の情報は受け手には伝達されても、その情報が正当なものであるとの認証までは出来ず、情報伝達が行われないという事態が発生する。これは、公証機関による公開鍵証明書を用いたとしても、その公開鍵証明書を真正な状態に維持できなければ、情報伝達の安全性は確保できない事を意味する。これを紙ベースの印鑑証明書に例えれば、証明すべき印鑑の印影が改ざんされれば、印鑑証明書の真正さが失われる事に相当する。

【０００６】

【課題を解決するための手段】そこで、本発明では、上記課題を解決し目的を達成するために、デジタル署名等の認証に利用する公開鍵暗号方式の少なくとも一対の公開鍵及び秘密鍵を、公開鍵及び該公開鍵に対する公証機関のデジタル署名とからなる公開鍵証明書と、秘密鍵とを、携帯可能情報記憶媒体として例えばＣＰＵ内蔵のＩＣカードに収容したものとして利用する。送り手は、このＩＣカードを保持管理し、必要な時にカードリーダライタにセットして使えば、不正に第三者にアクセスされる危険性はなくなる。また、このＩＣカードを用いた情報の認証方法は次の様にする。先ず、送り手は上記ＩＣカードを公証機関からオフラインで入手し、情報を受け手に送るときは、ＩＣカードに収容された秘密鍵でデジタル署名等の認証情報を作成し、この認証情報とＩＣカードに収容された公開鍵証明書とを、送付したい情報とともに送る。受け手では、別途公証機関から直接取得する等して用意した公証機関の公開鍵で、前記公開鍵証明書に含まれる送り手の公開鍵を認証し、認証された送り手の公開鍵と認証情報（例えばデジタル署名）で、送りてから送付された情報を認証する。また、送り手が受け手にネットワークで情報を送付する際に、情報に添付する認証情報に公開鍵暗号方式の公開鍵及び秘密鍵を用いる、認証システムとしては、送り手側での設備は上記ＩＣカードを（送り手自身の通信用コンピュータ或いは一時利用する通信用コンピュータに備えられたカードリーダライタに）セットしたものとし、送り手は、このＩＣカードの秘密鍵から認証情報を作成し、この認証情報とＩＣカードに収容された公開鍵証明書とを、情報と共に受け手に送付する。なお、受け手側では（単に情報を受け取り認証するのみならば）、公証機関の公開鍵を用意すれば良いので、上記の様なＩＣカードを設備したとしても、使う事はない。

【０００７】

【発明の実施の形態】以下、図面を参照しながら本発明の実施形態を説明する。先ず図２は、本発明の携帯可能情報記憶媒体の一例としてＩＣカードに一対の公開鍵及び秘密鍵が収容されている事の説明図である。公開鍵は、公証機関ＣＡの署名と共に公開鍵証明書という形態で収容される。携帯可能情報記憶媒体としては、改ざん防止という意味では、読出専用メモリに収容したＲＯＭカードとすることも可能であるが、安全性確保の為に秘密鍵の内容を外部に読み出せなくする、外部読出禁止属性を秘密鍵には設定しておくと良い。この点で、ＣＰＵを内蔵し、ＣＰＵ経由でアクセス権を制御するＩＣカードを用いると都合が良い。しかも、原文から暗号文への暗号化のプロセスは、ＩＣカードから秘密鍵を取り出して行うのでなく、ＩＣカードに原文を渡して、ＩＣカード内部で秘密鍵を用いて暗号文を作成出力することが、

ＣＰＵを内蔵することで可能となる。一方、公開鍵証明書は公表されるものであるから、読出禁止は意味がなく、改ざん防止を目的として、書換禁止属性を設定しておくと良い。

【０００８】本発明の携帯可能情報記憶媒体は、収容する公開鍵暗号方式の秘密鍵及び公開鍵は、メッセージ認証とユーザ認証を行うデジタル署名に用いるもの、或いはメッセージ認証に用いるもの等でも良い。なお、デジタル署名としてはＲＳＡ署名法に用いる秘密鍵及び公開鍵等である。また、メッセージ認証としては、冗長暗号化法等で用いる秘密鍵及び公開鍵等である。ところで、携帯可能情報記憶媒体中には、公開鍵が、公証機関のデジタル署名を伴った公開鍵証明書として収容されていることから、公証機関からオフラインで送り手に渡す。

【０００９】次に、以上の様な携帯可能情報記憶媒体を用いて行う、認証方法、認証システムについて説明する。図４は、送り手である太郎が、受け手である次郎に或るメッセージを送付するときに認証情報としてデジタル署名を行う際に、送付する情報の内容を説明する説明図である。太郎は、ＣＡ（公証機関）から秘密鍵と（太郎の公開鍵を有する）公開鍵証明書の入ったＩＣカードを取得しておく。太郎は、送りたいメッセージとＩＣカード中の秘密鍵とから署名を作成する。そして、メッセージと、署名と、ＩＣカードから公開鍵証明書を取り出して、これら三つを次郎に送る。なお、次郎側では、証明書の認証に用いるＣＡの公開鍵をＣＡから入手する。

【００１０】次に、図５は、次郎が受け取った情報から、太郎のメッセージを最終的に認証するまでの、手順の説明図である。先ず、次郎はＣＡの公開鍵で、送られた公開鍵証明書が真正であることを確認する。同図の矢印は、便宜上、ＣＡの公開鍵からＣＡの署名を認証し、ＣＡの署名から（太郎の）公開鍵を認証する様にしてあるが、図３によるデジタル署名の認証方法の説明、及びデジタル署名とはメッセージ認証とユーザ認証との両方の認証であることを踏まえれば、「ＣＡの署名の認証」（ユーザー認証）及び「（太郎の）公開鍵」の認証（メッセージ認証）とは、同時並列的に行われるものである。そして、認証された（太郎の）公開鍵で、（太郎の）署名を認証し、（太郎の）署名からメッセージを認証する。以上で、送られたメッセージが確かなもので有り、且つ太郎から送られたものであることを判断する。

【００１１】次に、図１は、以上の様な携帯可能情報記憶媒体、及び認証方法によって、ネットワークで認証を行う認証システムの説明図である。同図では、太郎が次郎にメッセージを送る際に、ＣＡ（公証機関）から秘密鍵等が収容された携帯可能情報記憶媒体としてＩＣカードを取得し、デジタル署名と、公開鍵証明書を添付して送る一例の説明である。同図のネットワークの認証システムでは、イーサネット等によるローカルエリアネットワークであり、公証機関の認証サーバー７には（太郎や次郎等の）公開鍵のデータベースが有り、さらにＩＣカード１０を発行する為のＩＣカードリーダライタ８を備えている。以下の説明例では、ＩＣカードの発行申請及び配付は郵送等のオフラインで行うので、この点では認証サーバーはネットワーク接続不要だが、次郎が公証機関自身の公開鍵を要求して入手するのはオンラインで行うので認証サーバーはネットワークに接続してあり、認証システムの一構成要素である。また、太郎及び次郎の端末９は、各人がそれぞれ自身の（秘密鍵等を収容した）ＩＣカードを持ち、メッセージにデジタル署名等を添付して送付できる様に、ＩＣカードリーダライタ８を備えている。

【００１２】① 先ず、最初のステップは、太郎から公証機関に公開鍵の登録申請を行う。同図では破線の矢印で示してある様に、この手続きはネットワークによらずに（オンラインでも良いが同図の場合は）郵送等のオフラインである。鍵はＲＳＡ署名法に用いる鍵で（秘密鍵及び公開鍵）である。公証機関は、申請を受けて、一対の鍵を生成し、公開鍵を公開鍵データベースに登録する。登録により、公証機関では太郎の公開鍵の正当性を保証でき、また重複発行を防止できる。登録するのは少なくとも公開鍵側のみで良い。なお、公証機関としては、その目的に応じて、例えば会社、都道府県単位の地方自治体、国などが役割を果たし得る。

【００１３】② 次のステップは、公証機関から太郎に、秘密鍵と、公開鍵及びその公開鍵に対する公証機関のデジタル署名を有する公開鍵証明書とを有する、ＩＣカードを、郵送等のオフラインで送付する。この過程で、太郎の公開鍵に対する証明書も、前記ＩＣカードに入れて太郎に送ってしまう。

【００１４】③ そして、太郎は次郎に、太郎のデジタル署名付きのメッセージを、公開鍵証明書とともに、ネットワークで送る。太郎はＩＣカードリーダライタに自分のＩＣカードをセットする。デジタル署名の作成方法は、先に説明した通りであり、秘密鍵を引出して、或いはＩＣカード内部で暗号化する等して作成する。なお、ＩＣカード自身を盗難された場合に悪用を防ぐために、収容された秘密鍵の使用、及び公開鍵証明書の読み出し等は、所有者のパスワードを設定しておけば良い。

【００１５】④ 一方、メッセージを送られた次郎側では、公開鍵証明書を真正なものであることを認証するために、該証明書にある公証機関のデジタル署名を認証する為の、公証機関の公開鍵を、送付された後又は前でも良いが、用意しておく必要がある。（同一の公証機関の公開鍵を既に他の認証で入手済みならば、それを使用できる。）

次郎が公証機関の公開鍵を入手する方法、同図の例の場合はオンラインで公証機関に公証機関の公開鍵を要求し、公証機関はオンラインで次郎に公証機関の公開鍵を送付する。なお、公証機関から次郎への公証機関の公開

鍵の送付は、該公開鍵がその公証機関のものに間違いない事を証明する、公開鍵の証明書として送付する。この証明書は、該公証機関よりもより上位の上位公証機関で発行されたもので、下位公証機関の公開鍵と、該公開鍵に対する上位公証機関のデジタル署名とからなる、公証機関の公開鍵に対する証明書である。公証機関の上位、下位とは、例えば、会社に対しては地方自治体、地方自治体に対しては国等といった具合である。なお、公証機関の公開鍵を、太郎の公開鍵に対する（太郎の）公開鍵証明書と同様に、（公証機関の）公開鍵証明書として送付するのは、公表する公開鍵の改ざんを防ぐ為である。以上の様にして、公証機関の公開鍵を証明書として入手した次郎は、別途入手した上位公証機関の公開鍵で、その証明書を認証して、公証機関の公開鍵を確かに入手する。

【００１６】⑤　そして、次郎は、入手した公証機関の公開鍵で、太郎から送られた公開鍵証明書にあった公証機関のデシダル署名を認証し、太郎の公開鍵を認証する。

⑥　次いで、次郎は、認証した太郎の公開鍵で、太郎のメッセージを認証する。

【００１７】

【発明の効果】本発明によれば、認証に利用する秘密鍵及び公開鍵、さらに公証機関による公開鍵の証明書を安全に管理できる。これらを収容する携帯可能情報記憶媒体において、秘密鍵を外部読出禁止属性とし媒体内部で暗号化したり、公開鍵証明書を書換禁止属性とすることで、より安全に鍵の管理ができる。なお、これら属性の設定には、ＣＰＵを内蔵するＩＣカードを用いる。また、携帯可能情報記憶媒体中に鍵等が保管されているので、自分のネットワーク端末の磁気ディスク内等にこれら鍵等を保管する必要がなく、端末が他人に使用されて磁気ディスクに保管された鍵等を不正に盗用された、改ざんされる恐れが無い。携帯可能情報記憶媒体は、必要な時のみ端末のカードリーダライタにセットしておけば良く、後は自分で所持管理しておれば良い。従って、他のネットワーク端末でもこの携帯可能情報記憶媒体をセットすれば、情報を安全に送ることができる。また、鍵を磁気ディスクに収容して利用する従来の場合では、磁気ディスクに収容された状態を時間的に少なくする事で盗用や改ざんを防止する目的で、鍵が必要になる都度、公証機関に問い合わせして鍵を入手する使い方が望ましかった。しかし、本発明では、携帯可能情報記憶媒体内に安全に鍵を管理できるので、送り手側は毎回公証機関に毎回問い合わせする必要がなく、公証機関側としても最初に一回だけ携帯可能情報記憶媒体を本人に渡してしまえば済み、公証機関側での鍵運営も効率化できる。

【図面の簡単な説明】

【図１】本発明の携帯可能情報記憶媒体を用いた認証システム、認証方法の説明図。

【図２】本発明の携帯可能情報記憶媒体が有する情報及び機能の一例の説明図。

【図３】デジタル署名の説明図。

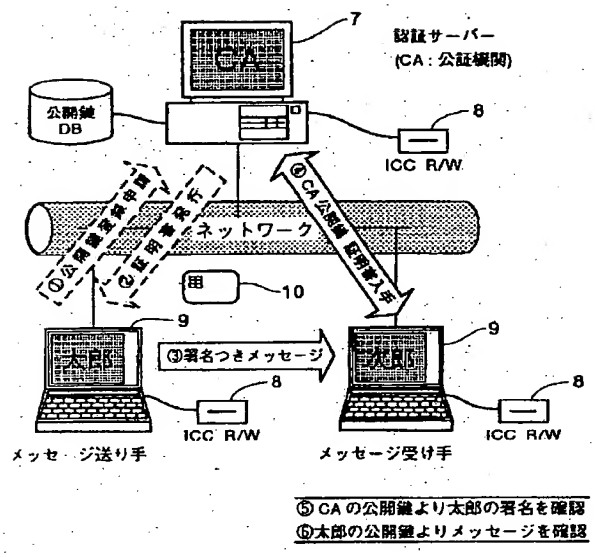
【図４】本発明による情報伝達内容の説明図。

【図５】本発明による受け手側での認証の手順の説明図。

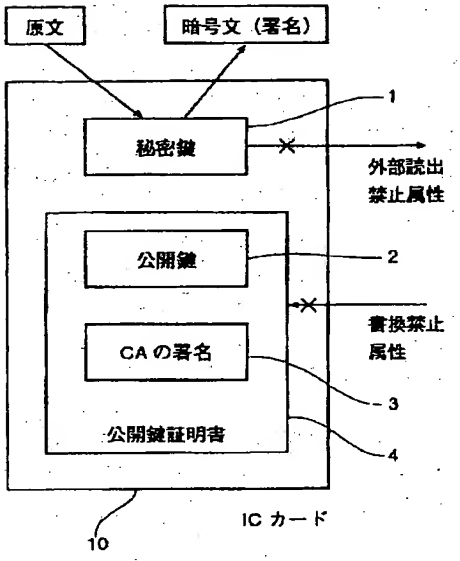
【符号の説明】

１　秘密鍵
２　公開鍵
３　ＣＡのデジタル署名
４　公開鍵証明書
５　原文（メッセージ等）
６　暗号文（デジタル署名等）
７　認証サーバー
８　カードリーダライタ
９　端末
１０　携帯可能情報記憶媒体（ＩＣカード等）

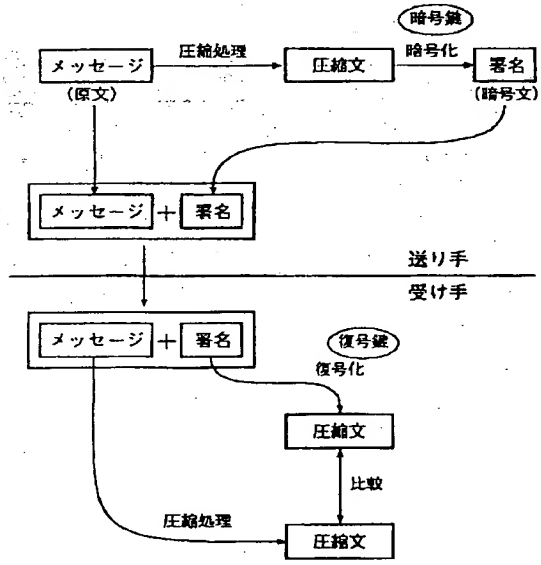
【図1】


認証サーバー
(CA：公証機関)
CA
公開鍵
DB
7
8
ICC R/W
ネットワーク
10
9
太郎
次郎
③署名つきメッセージ
メッセージ送り手
メッセージ受け手
⑤CAの公開鍵より太郎の署名を確認
⑥太郎の公開鍵よりメッセージを確認

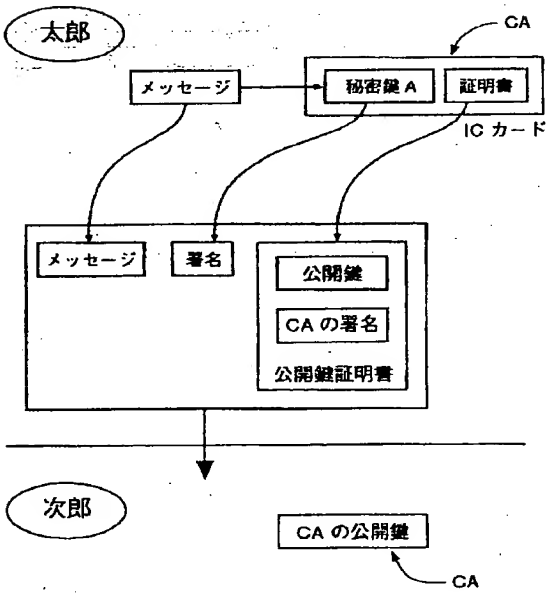
【図2】


原文
暗号文（署名）
秘密鍵
1
外部読出
禁止属性
公開鍵
2
CAの署名
3
書換禁止
属性
公開鍵証明書
4
ICカード
10

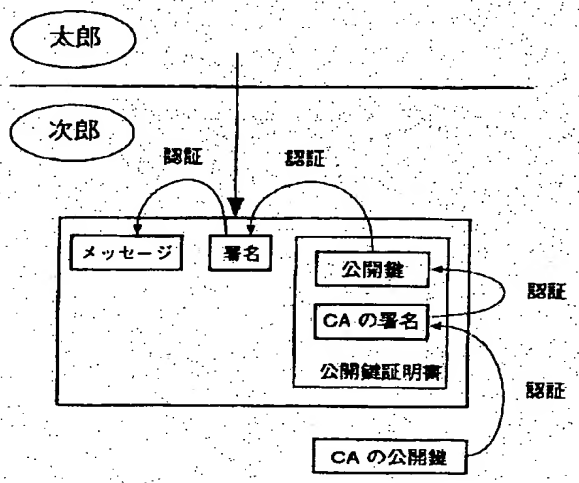
【図3】


暗号鍵
メッセージ
(原文)
圧縮処理
圧縮文
暗号化
署名
(暗号文)
メッセージ
署名
送り手
受け手
メッセージ
署名
復号鍵
復号化
圧縮文
比較
圧縮処理
圧縮文

【図4】


太郎
CA
メッセージ
秘密鍵A
証明書
ICカード
メッセージ
署名
公開鍵
CAの署名
公開鍵証明書
次郎
CAの公開鍵
CA

【図5】



フロントページの続き

(51)Int.Cl.[6]		識別記号	庁内整理番号	FI		技術表示箇所
G09C	1/00	660	7259－5J	G09C	1/00	660A
H04L	9/32			H04L	9/00	675B
// G07F	7/08			G07F	7/08	Z